frontiers | Frontiers in Energy Research

TYPE Original Research
PUBLISHED 23 January 2023
DOI 10.3389/fenrg.2022.1082442

A dynamic game model for assessing risk of coordinated physical-cyber attacks in an AC/DC hybrid transmission system

Xuecheng Liu and Libao Shi*

National Key Laboratory of Power Systems in Shenzhen, Shenzhen International Graduate School, Tsinghua University, Shenzhen, China

Check for updates

OPEN ACCESS

EDITED BY
Zhiyi Li,
Zhejiang University, China

REVIEWED BY
Jiwei Tian,
Air Force Engineering University, China
Junjun Xu,
Nanjing University of Posts and Telecommunications, China

*CORRESPONDENCE
Libao Shi,
shilb@sz.tsinghua.edu.cn

SPECIALTY SECTION
This article was submitted to Smart Grids, a section of the journal Frontiers in Energy Research

RECEIVED 28 October 2022
ACCEPTED 25 November 2022
PUBLISHED 23 January 2023

CITATION
Liu X and Shi L (2023), A dynamic game model for assessing risk of coordinated physical-cyber attacks in an AC/DC hybrid transmission system.
Front. Energy Res. 10:1082442.
doi: 10.3389/fenrg.2022.1082442

COPYRIGHT
© 2023 Liu and Shi. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.

The widely used intelligent measuring equipment not only makes the operation of AC/DC hybrid transmission system more safe and reliable, but also inevitably brings new problems and challenges such as the threats and hidden dangers of cyber attacks. Given this, how to effectively and comprehensively assess the inherent vulnerabilities of AC/DC hybrid transmission systems under the coordinated physical-cyber attacks is of critical significance. In this paper, a three-stage physical-cyber attack and defense risk assessment framework based on dynamic game theory is proposed. In the framework, the dynamic game process between attacker and defender is carried out for the power grid risk, which is expressed as the product of the attacker's success probability in attacking the substation and the load loss caused by the attack. Regarding the probability of a successful attack, it depends on the number of funds invested by both attacker and defender sides considering the marginal effect, while the corresponding load loss caused depends on the cyber attack vector and the optimal load shedding scheme. For the solution of the proposed three-stage dynamic game framework, it is converted into a bi-level mathematical programming problem, in which the upper-level problem is solved by using the backward induction method to get the subgame perfect Nash equilibrium, and the lower-level problem is solved by using an improved particle swarm optimization algorithm to get the optimal amount of load shedding. Finally, the case study is performed on a modified IEEE 14-node AC/DC hybrid transmission test system, and the inherent weaknesses of the power grid are identified based on the risk assessment results, verifying the effectiveness of the proposed framework and method.

KEYWORDS

AC/DC hybrid transmission system, false data injection attack, game theory, Nash equilibrium, risk assessment

1 Introduction

With the continuous evolution and in-depth integration of the physical power grid composed of practical equipment and the advanced information communication system (ICS), a powerful cyber physical power system (CPPS) has been gradually formed. In particular, with the deep interaction between the physical power grid and ICS, the high dependence of the power grid on the measurement data will cause great damage to the power system security and stability under cyber attacks that compromise the availability, integrity, and confidentiality of power grid data (Xu et al., 2021). Compared with physical attacks, some cyber attacks, such as the false data injection (FDI) and distributed denial of service (DDoS) attacks, are highly stealthy, easy to implement, and difficult to defend promptly. It is known that the blackout occurred in Ukraine on 23 December 2015 was the first event in the world that was considered as a malicious cyber attack on the power supply system (Liang et al., 2016). In the blackout, a malware called "Black Energy" attacked 60 substations roughly, resulting in power outage of 1.4 million people in western Ukraine for 3–6 h. Thereafter, more and more cyber attacks have occurred in power systems around the world, and have caused certain system losses and social impact, such as the ransomware attack on the Israeli national grid in 2016 and the satellite DoS attack on a German wind farm in 2022. As a result, it is foreseeable that as more and more intelligent devices are put into the modern AC/DC hybrid transmission system, especially with the increasing proportion of large-scale grid-connected clean energy and energy storage system, once the power grid suffers from the coordinated physical-cyber attacks, it will cause inestimable and severe economic and social losses, affecting people's normal life.

So far, a lot of research has been conducted on the risk analysis of CPPS in the case of cyber attacks. Regarding the interactions between cyber attackers and power grid defenders, a bi-level optimization problem has been constructed to perform vulnerability analysis (Yuan et al., 2011; Khanna et al., 2017), in which the upper level problem mainly described the behavior of the attacker, while the lower level problem mainly achieved the power grid protection based on security-constrained economic dispatch. In (Che et al., 2018), a cyber-secured corrective dispatch scheme was proposed to protect the power grid from potential data attacks. In (Chung et al., 2018), a coordinated cyber-physical attack scheme was proposed to cause more serious consequences, and a target selection criterion was designed to achieve higher attack success rate. The bi-level optimization model built in the above studies mainly focuses on the behavior of attackers and defenders, ignoring the impact of resource deployment on attack and defense, which can help attackers gain access to key equipment through related vulnerabilities to achieve the purpose of attack or help defenders detect attack behavior through related defense facilities to ensure the security of the power grid. In order to better describe the resource allocation between attackers and defenders, many studies have used game frameworks to model the strategic choices of attacks and defenses, that is, the choice of various resource allocation schemes (Ranjbar et al., 2019; Dai and Shi, 2020; Gao and Shi, 2020; Hasan et al., 2020; Shan and Zhuang, 2020; Zhang et al., 2021). In addition, different game models have been used to explain a variety of attack and defense scenarios according to the research target and cyber attack methods. In Xiang et al. (2018), a system adequacy evaluation framework incorporating cyber attacks and physical failures was proposed to quantify the influence of cyber attacks on the power supply adequacy, and the static and Markov games were applied to model the interactions between defenders and attackers. In Wang et al. (2017), a Bayesian honeypot game strategy was introduced to investigate the DDoS attack in the advanced metering infrastructure network, and the interactions between the defenders and the attackers were analyzed elaborately. In Liu and Wang (2021), a FlipIt game model was established to investigate the interactions between the defender, the attacker and insider, and three types of insiders and their corresponding impacts on the supervisory control and data acquisition system were modeled and analyzed. In Lakshminarayana et al. (2021), a zero-sum non-cooperative game model was proposed to find the optimal placement of distributed flexible AC transmission system as defense resource, so as to realize a moving target defense strategy against the coordinated physical-cyber attack. In order to study the interactions between defenders and attackers more comprehensively, two game models, namely a Stackelberg game and a hybrid satisfaction equilibrium-Nash equilibrium game, were applied to study the impacts of data injection attacks on the smart grid with multiple adversaries taken into account (Sanjab and Saad, 2016). In Wei et al. (2016), a stochastic game-theoretic approach was proposed to find the optimal strategy of defender to protect the power grid against coordinated physical-cyber attack. Although these game models mentioned above explained the interaction of the resource allocation between attackers and defenders in detail, the risks of power system, usually quantified as the product of the attack success probability and the corresponding consequences, still needs to be studied in-depth. The classic three-stage defender-attacker-defender dynamic game models with complete information were proposed to assess the operation risks of transmission lines (Gao and Shi, 2020) and feeder automation system (Dai and Shi, 2020) under various physical-cyber attack scenarios. In Zhang et al. (2021), a zero-sum multi-level Markovian Stackelberg game was proposed to model the sequential attack and defense actions on both cyber layer and physical layer, aiming to mitigate the risks of power system. Moreover, some studies also conducted risk analysis on CPPS system based on game theory by considering the information asymmetry between attackers and defenders (Gao et al., 2019; Wang et al., 2019; Shao and Li, 2021; Tian et al., 2021). In the aforementioned existing studies, almost all the studies are conducted for the AC transmission systems, and few studies investigate and discuss the impact of cyber attacks on the AC/DC hybrid transmission systems. In Amir et al. (2019), the impacts of the cyber-attacks on the HVDC system and the effects on the dynamic voltage stability were investigated to implement the cyber-physical vulnerability and security evaluation of AC/DC hybrid power grid. In Qiu et al. (2021), a HVDC ancillary control strategy based on a hybrid data-driven technology was proposed to effectively improve the controllability of the HVDC intertie under the FDI attacks. Although the existing work on the impact of cyber attacks on power grid operation and stability has achieved fruitful research results using models and methods with varying degrees of detail, the resource allocation of defenders and attackers is relatively abstract, lacking some practical significance, and the attack and defense strategies adopted are difficult to reflect the actual operating conditions of the power grid studied. Meanwhile, most of the existing work takes the implementation conditions of the cyber attacks as the main factor affecting the success probability of cyber attacks, such as whether the false data can pass the bad data detection in the FDI attacks, lacking the modeling of the specific process of cyber attacks, which obviously will affect the success probability of attackers. In addition, most of the existing research work mainly focuses on the AC transmission systems, but the operation risk of the AC/DC hybrid transmission system under the coordinated physical-cyber attacks is rarely discussed. More intensive and specific research work needs to be further carried out to model the resource allocation of attackers and defenders, and the cyber attack process and the corresponding risk assessment of AC/DC hybrid system need to be explored and exploited in more detail.

In this paper, a three-stage dynamic game risk assessment framework for an AC/DC hybrid transmission system under the coordinated physical-cyber attacks is proposed, and then this three-stage dynamic game framework is converted into a bi-level mathematical optimization problem, which is solved by using the backward induction (BI) method and an improved particle swarm optimization (IPSO) algorithm. The main contributions of this paper are summarized in the following three-fold.

1) A three-stage physical-cyber attack and defense risk assessment framework based on dynamic game theory is proposed, aiming to effectively identify the inherent vulnerability of the AC/DC hybrid transmission system under the coordinated physical-cyber attacks.
2) The process of substation suffering from the cyber and physical attacks is elaborately modeled to implement the quantification of the actual success probability of the FDI attack on the substation, which lays the foundation for the risk assessment of the system.
3) A FDI attack model, targeting the AC/DC hybrid transmission system, is carefully constructed based on AC state estimation to bypass the bad data detector and effectively realize more stealthy cyber attacks. In addition, an IPSO algorithm is applied to solve the proposed FDI attack model with highly non-linear characteristics.

The structure of the paper is organized as follows. In Section 2, a three-stage physical-cyber attack and defense risk assessment framework based on dynamic game theory is discussed. The corresponding solution methodology based on the BI and an IPSO algorithms is given in Section 3. The case study based on a modified IEEE 14-node test system is performed in Section 4. Finally, Section 5 concludes this paper and discusses possible future work.

2 Problem formulation

In this paper, a dynamic game framework is proposed to conduct the risk assessment of coordinated physical-cyber attacks in an AC/DC hybrid transmission system. In this dynamic game framework, two players are involved, namely an attacker and a defender. The attacker is assumed to be an attack team that consists of hackers, mainly performing data monitoring and cyber attacks against substations, and the FDI attacks are used as the main means of cyber attacks. The defender is also assumed to be a defensive team that consists of utility managers, substation inspectors, and cyber security technicians. The defensive team aims at reducing the success probability of cyber attacks on the transmission system by improving inspection efforts and identifying network vulnerabilities, and on the other hand, the defensive team will also conduct optimal load shedding strategy after being attacked. Based on game theory, and according to the action sequence of game participants, this paper proposes a three-stage physical-cyber attack and defense risk assessment framework for an AC/DC hybrid transmission system. The corresponding dynamic game equilibrium solution can not only obtain the optimal attack and defense strategies, but also identify the inherent weaknesses of the power grid according to the risk assessment results.

Figure 1 illustrates the game process of the three-stage physical-cyber attack and defense. In stage 1, the defender allocates limited defense funds to protect the cyber security and physical security of the substation. In stage 2, the attacker allocates limited attack funds to conduct cyber attacks on the substation, and gains the right to tamper with power grid data by performing FDI attacks. In stage 3, the defender adopts the optimal load shedding scheme for the AC/DC hybrid transmission system to minimize the power grid risk.

The following basic assumptions are listed in modeling the proposed three-stage dynamic game framework.

1) The topology and all parameters of the power system are accessible to the attacker.
2) The defense strategies employed by the defender, namely the allocation of cyber defense and physical defense funds, are exposed to the attacker.

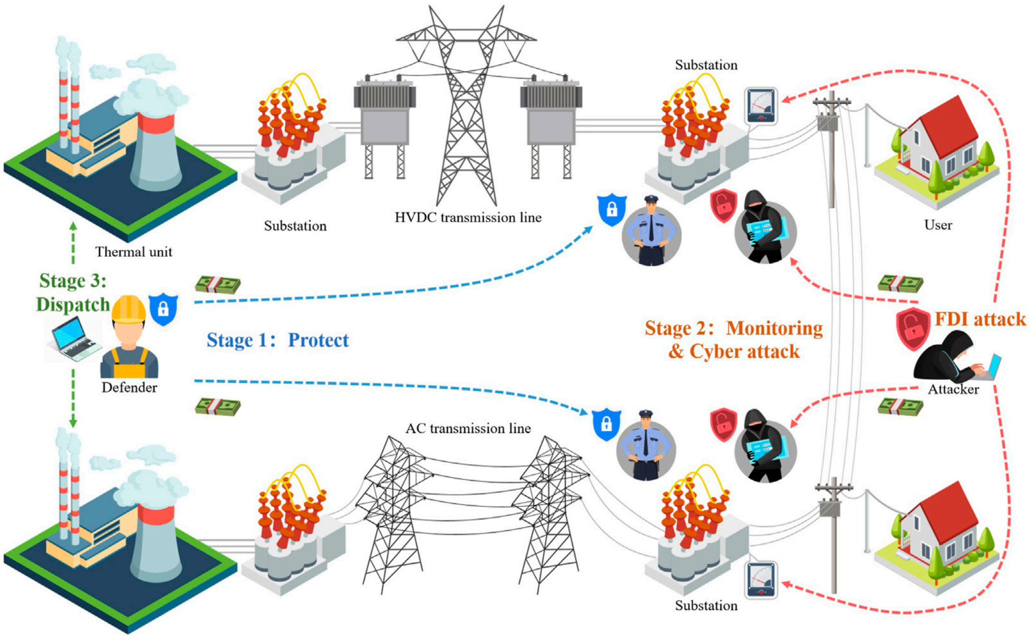


FIGURE 1
Illustration of three-stage physical-cyber attack and defense in an AC/DC hybrid transmission system.

3) The attacker knows the optimal load shedding scheme that the defender will take if the attacks succeed.
4) The defender will consider the strategies of attackers before allocating defense funds.

Accordingly, the "defender-attacker-defender" three-stage game model established in this paper is a dynamic game with perfect information.

In order to further quantitatively evaluate the power grid risk under the coordinated physical-cyber attacks, a power grid attack risk index (*GARI*) is defined as follows, also representing the payoffs to the attacker and defender.

$$\min_{d\in SD}\ \max_{a\in SA(d)}\ \min_{l\in SL(d,a)} GARI(d,a,l) \tag{1}$$

In this paper, the proposed *GARI* is computed as the product of the vulnerability of the substation under coordinated physical-cyber attacks and the corresponding consequences caused, which is expressed as

$$GARI(d,a,l) = V(d,a)\cdot C(l) \tag{2}$$

2.1 Stage 1: Deployment of defense funds

Regarding the cyber side, the defender can reduce the success probability of cyber attacks against substations by upgrading software, performing routine security checks, and purchasing data monitoring equipment. Especially in view of the fact that each substation improves its own communication network by applying for funds from the utility, and that there is an upper limit on these funds, a discrete allocation scheme of funds is designed in this paper to represent the deployment of defense funds, which is modeled as follows:

$$\begin{cases} S_{Cyd} = \{Cyd_i\} \\ \sum_{i\in B} Cyd_i \le F_{Cyd}, Cyd_i \in \{0, CydL_1, CydL_2\}, Cyd_i \ge 0 \end{cases} \tag{3}$$

Regarding the physical side, the defender needs to prevent attacker from bribing substation staff and investigate the illegally installed monitoring devices around the substation to be attacked. Similarly, a discrete allocation scheme of defense funds is given as follows:

$$\begin{cases} S_{Phd} = \{Phd_i\} \\ \sum_{i\in B} Phd_i \le F_{Phd}, Phd_i \in \{0, PhdL_1, PhdL_2\}, Phd_i \ge 0 \end{cases} \tag{4}$$

The set of defense fund deployment strategies for the defender can be determined after considering the allocation of funds for both cyber defense and physical security, which is given as follows:

$$SD = \left\{d \middle| d = \left(S_{Cyd}, S_{Phd}\right)\right\} \tag{5}$$

2.2 Stage 2: Deployment of attack funds

As mentioned above, the main form of cyber attacks launched by attackers on the cyber side is the FDI attacks. In order to meet the conditions under which the FDI attacks can be performed, the attack team must hire a certain number of hackers to infiltrate the cyber network and falsify data. In this paper, it is assumed that the attack team pays different hacking service fees according to the skill level of the hired hackers. In view of this, a discrete hacking service fee scheme is designed to model the deployment of attack funds on cyber side, which is expressed as

$$\begin{cases} S_{Cya} = \{Cya_i\} \\ \sum\limits_{i \in A} Cya_i \le F_{Cya}, Cya_i \in \{CyaL_1, CyaL_2\}, Cya_i > 0 \end{cases} \tag{6}$$

To improve the success probability of performing FDI attacks against the AC/DC hybrid transmission system, it is essential to obtain some corresponding information of power grid, such as network topology and power flow data. More importantly, once the attack team obtains the SSH port number and password of measuring equipment in the target substations, it will be very easy to execute a stealthy FDI attack. Therefore, the attack team will spend certain funds to obtain power grid information by bribing substation staff and illegally installing some monitoring devices. Similarly, a discrete monitoring fee scheme is designed to model the deployment of attack funds on the physical side, which is expressed as

$$\begin{cases} S_{Pha} = \{Pha_i\} \\ \sum\limits_{i \in A} Pha_i \le F_{Pha}, Pha_i \in \{PhaL_1, PhaL_2\}, Pha_i > 0 \end{cases} \tag{7}$$

The set of attack fund deployment strategies for the attacker can be determined after considering the allocation of funds for both cyber attacks and physical monitoring, which is given as follows:

$$SA = \left\{ a \middle| a = \left(S_{Cya}, S_{Pha}\right) \right\} \tag{8}$$

Once two players, the defender and the attacker, have deployed funds in sequential order, the probability of a successful cyber attack can be determined. Regarding the attack on the cyber side, the probability of an attacker successfully attacking the i^{th} substation consists of the following two items:

$$p_{Cy,i} = p_{BAG,i} \cdot p_{con,i} \tag{9}$$

In this paper, the probability $p_{BAG,i}$ can be calculated by using a Bayesian attack graph model as shown in Figure 2, which can clearly indicate the path of the cyber attack.

In Figure 2, the hackers exploit the vulnerabilities < SSH1, 2>, <log2,3>, and <DB 3,4>, respectively, and get the control right of the substation, namely the right of User (4) in accordance with the <1,2>, <2,3>, and <3,4 > connectivity paths. The corresponding details of each vulnerability are shown in Table 1, and the value of each vulnerability can be calculated quantitatively based on the common vulnerability scoring system (CVSS) (National institute of standards and technology, 2022), which is a method used to provide qualitative measure of severity. In addition, the CVSS also provides a lot of information about each vulnerability, such as impact, attack vector, weakness, or other relevant technical information. The given information can help determine the number from 0 to 10 as the CVSS score, and the larger the number, the higher the severity of the vulnerability.

The final success probability of an attacker falsifying the data of the i^{th} substation can be obtained from the attack path given in Figure 2, which is modeled as

$$p_{BAG,i} = p(\mathrm{SSH}) \cdot p(\mathrm{Log}) \cdot p(\mathrm{DB}) \tag{10}$$

In this paper, the CVSS score is divided by 10 to implement the normalization as the success probability of a cyber attack, so the $p(\mathrm{SSH})$, $p(\mathrm{Log})$, and $p(\mathrm{DB})$ are defined as 8%, 55% and 78%, respectively.

For the connectivity probability $p_{con,i}$, for simplicity, it can be expressed as follows, in which it is assumed that the marginal effect of the funds invested by both the attacker and defender is taken into account:

$$p_{con,i} = 0.9e^{-\frac{Cyd_i}{\mu + Cya_i}} + 0.1 \tag{11}$$

It should be noted that the value of μ is related to the number of measurement devices installed in the substation.

Regarding the attack on the physical side, the attacker can not only obtain the basic information of the power grid by monitoring data or bribing staff, but also obtain SSH port information and password of substation. Therefore, we propose the following expression to model the probability of obtaining SSH port and password by non-network intrusion means $p_{Ph,i}$ with the marginal effect taken into account:

$$p_{Ph,i} = \frac{Pha_i}{\lambda + Pha_i} \cdot \frac{\lambda}{\lambda + Phd_i} \tag{12}$$

It should be noted that the value of λ is related to the strength of the substation security forces.

To sum up, the actual success probability of the FDI attack on the i^{th} substation can be expressed as

$$p_i = \frac{2\arctan\left(p_{Cy,i} + p_{Ph,i} \cdot p(DB) \cdot p_{con,i}\right)}{\pi} \tag{13}$$

More specifically, the success probability of the attacker's FDI attack on the AC/DC hybrid transmission system is the cumulative product of the success probability of the attack on all target substations, which can also be referred to the vulnerability of the power grid under cyber attacks $V(d, a)$ given as follow:

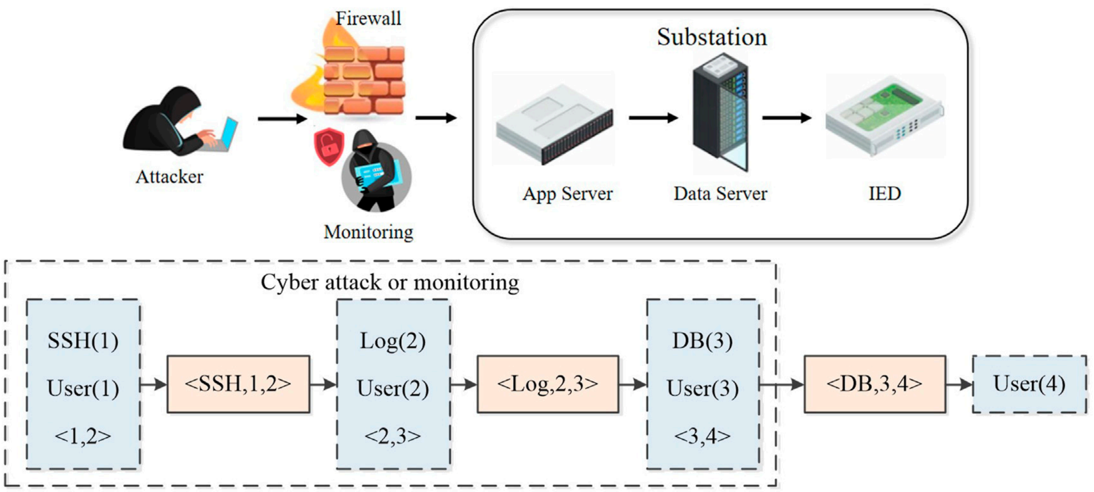


FIGURE 2
Bayesian attack graph model of substation under cyber attack.

TABLE 1 Information on the vulnerabilities exploited during the attack.

Vulnerability	CVSS	Description
<SSH, 1,2>	0.8	Get the port number for remote control
<Log,2,3>	5.5	Weak password authentication
<DB, 3,4>	7.8	Obtain read and write access to the database

$$V(\boldsymbol{d},\boldsymbol{a}) = \prod_{i\in A} \boldsymbol{p}_i \tag{14}$$

2.3 Stage 3: Defender's action

In the Stage 1 and Stage 2, once the deployment strategies of defense and attack funds are determined, the vulnerability of the substation attacked $\boldsymbol{V}(\boldsymbol{d},\boldsymbol{a})$ given in (Eq. 2) becomes a constant term, and the aforementioned *GARI* can be rewritten as

$$\boldsymbol{GARI}(\boldsymbol{d}',\boldsymbol{a}',\boldsymbol{l}) = \boldsymbol{V}(\boldsymbol{d}',\boldsymbol{a}')\cdot\boldsymbol{C}(\boldsymbol{l}) \tag{15}$$

In this situation, the defender only needs to take some actions in response to the consequence $\boldsymbol{C}(\boldsymbol{l})$ in Stage 3. In this paper, the following max-min optimization problem is proposed to model the consequence $\boldsymbol{C}(\boldsymbol{l})$:

$$\boldsymbol{C}(\boldsymbol{l}) = \max_{ATK}\ \min_{DEF} \sum_{\Delta P_{dL}\in DEF} \Delta P_{dL},\ \boldsymbol{l} = (\boldsymbol{ATK},\boldsymbol{DEF}) \tag{16}$$

Since the target of FDI attacks in this paper is the AC/DC hybrid transmission system, the attacker constructs the attack vectors based on AC state estimation to bypass the bad data detector in EMS system. Inspired by the existing FDI attack modeling for AC state estimation (Rahman and Mohsenian-Rad, 2013; Liu and Li, 2016), the corresponding FDI attack vector set $\boldsymbol{ATK}$ is indicated as

$$\boldsymbol{ATK} = (\Delta\boldsymbol{P}_{dA},\Delta\boldsymbol{Q}_{dA},\Delta\boldsymbol{V}_{mA},\Delta\boldsymbol{\theta}_A) \tag{17}$$

It should be noted that since the measurement devices in substation cannot measure the phase angle, so the actual attack vector does not contain $\Delta\boldsymbol{\theta}_A$, which is listed here only to indicate the integrity of the constraint variables. Moreover, the number of attacked substations corresponding to the FDI attack vector cannot exceed $\boldsymbol{nATK}_{max}$ to ensure the invisibility of FDI attacks.

To ensure that the FDI attack based on AC state estimation can bypass the bad data detector, the attacker must obey the following rules:

1) The voltage magnitude of the generator node cannot be modified;
2) Only the voltage magnitude and phase angle of the zero-load node can be modified;
3) The voltage magnitude and phase angle of the node adjacent to non-attacked nodes (called edge nodes) cannot be modified;
4) The variation of all tampered data should be within a certain range;
5) The data of DC transmission lines cannot be tampered with.

Based on these rules described above, the FDI attack constraints are indicated as follows:

$$\begin{cases}-\tau P_{d,i} \le \Delta P_{dA,i} \le \tau P_{d,i} \quad (i \in A) \\ -\tau Q_{d,i} \le \Delta Q_{dA,i} \le \tau Q_{d,i} \quad (i \in A) \\ -\tau V_{m,i} \le \Delta V_{mA,i} \le \tau V_{m,i} \quad (i \in A) \\ -\tau \theta_i \le \Delta \theta_{A,i} \le \tau \theta_i \quad (i \in A) \\ \Delta V_{mA,k} = 0 \quad (k \in A_g) \\ \Delta P_{dA,k} = 0 \quad (k \in A_0) \\ \Delta Q_{dA,k} = 0 \quad (k \in A_0) \\ \Delta V_{mA,k} = 0 \quad (k \in A_e) \\ \Delta \theta_{A,k} = 0 \quad (k \in A_e) \\ PartLF\left(P_d + \Delta P_{dA}, Q_d + \Delta Q_{dA}, V_m + \Delta V_{mA}, \theta + \Delta \theta_A, P_{gA}, Q_{gA}\right) = 0 \end{cases} \tag{18}$$

The corresponding ***PartLF*** constraints are specified as

$$\begin{cases} P_i = V_{m,i} \sum_{j=1}^{nA} V_{m,j}\left[g_{ij} \cos(\theta_i - \theta_j) + b_{ij} \sin(\theta_i - \theta_j)\right] \quad (i,j \in A) \\ Q_i = -V_{m,i} \sum_{j=1}^{nA} V_{m,j}\left[b_{ij} \cos(\theta_i - \theta_j) - g_{ij} \sin(\theta_i - \theta_j)\right] \quad (i,j \in A) \\ P_i = P_{g,i} - P_{d,i} - \Delta P_{dA,i} + P_{leq,i} \quad (i \in A) \\ Q_i = Q_{g,i} - Q_{d,i} - \Delta Q_{dA,i} + Q_{leq,i} \quad (i \in A) \\ P_{leq,i} = 0 \quad (i \notin A_e) \\ Q_{leq,i} = 0 \quad (i \notin A_e) \end{cases} \tag{19}$$

Similar to the FDI attack vector, the optimal load shedding vector set ***DEF*** for the AC/DC hybrid transmission system can be indicated as

$$DEF = (\Delta P_{dL}, \Delta Q_{dL}) \tag{20}$$

Subject to the following constraints:

$$\begin{cases} 0 \le \Delta P_{dL,i} \le P_{d,i} \quad (i \in B) \\ \left|\Delta Q_{dL,i}\right| \le \left|Q_{d,i}\right|, \Delta Q_{dL,i} \cdot Q_{d,i} \ge 0 \quad (i \in B) \\ V_{m\min,i} \le V_{m,i} \le V_{m\max,i} \quad (i \in B) \\ \theta_{\min,i} \le \theta_i \le \theta_{\max,i} \quad (i \in B) \\ S_{l,ij} \le S_{l\max,ij} \quad (i,j \in B) \\ P_{g\min,i} \le P_{g,i} \le P_{g\max,i} \quad (i \in B) \\ Q_{g\min,i} \le Q_{g,i} \le Q_{g\max,i} \quad (i \in B) \\ LF\left(P_d + \Delta P_{dA} - \Delta P_{dL}, Q_d + \Delta Q_{dA} - \Delta Q_{dL}, V_m, \theta, P_g, Q_g\right) = 0 \end{cases} \tag{21}$$

The corresponding ***LF*** constraints are specified as

$$\begin{cases} P_i = V_{m,i} \sum_{j=1}^{nB} V_{m,j}\left[g_{ij} \cos(\theta_i - \theta_j) + b_{ij} \sin(\theta_i - \theta_j)\right] \quad (i,j \in B) \\ Q_i = -V_{m,i} \sum_{j=1}^{n} V_{m,j}\left[b_{ij} \cos(\theta_i - \theta_j) - g_{ij} \sin(\theta_i - \theta_j)\right] \quad (i,j \in B) \\ P_i = P_{g,i} - P_{d,i} - \Delta P_{dA,i} \quad (i \in A) \\ Q_i = Q_{g,i} - Q_{d,i} - \Delta Q_{dA,i} \quad (i \in A) \\ P_i = P_{g,i} - P_{d,i} \quad (i \notin A) \\ Q_i = Q_{g,i} - Q_{d,i} \quad (i \notin A) \end{cases} \tag{22}$$

In this paper, the line commutated converter (LCC) model as shown in Figure 3 is applied to formulate the HVDC transmission line, which is given as follows (Kundur and Malik, 2022):

$$\begin{cases} U_d' = \frac{3\sqrt{2}}{\pi} n' U' \cos\alpha - \frac{3}{\pi} X_C' I_d \quad (\text{Rectifier}) \\ U_d'' = \frac{3\sqrt{2}}{\pi} n'' U'' \cos\gamma - \frac{3}{\pi} X_C'' I_d \quad (\text{Inverter}) \\ \cos\varphi' = \dfrac{U_d'}{\frac{3\sqrt{2}}{\pi} n' U'} \quad (\varphi' \in \text{I Quadrant}) \\ \left|\cos\varphi''\right| = \dfrac{U_d''}{\frac{3\sqrt{2}}{\pi} n'' U''} \quad (\varphi'' \in \text{II Quadrant}) \\ P_d' = U_d' I_d \quad (>0), \ Q_d' = P_d' \tan\varphi' \quad (>0) \\ P_d'' = -U_d'' I_d \quad (<0) \ Q_d'' = \left|P_d'' \tan\varphi''\right| \quad (>0) \\ \theta_I' = \theta_U' - \varphi', \ \theta_I'' = \theta_U'' - \varphi'' \\ I' = \frac{\sqrt{6}}{\pi} n' I_d, I'' = \frac{\sqrt{6}}{\pi} n'' I_d, R_d I_d = U_d' - U_d'' \end{cases} \tag{23}$$

By solving the optimization problem shown in (Eq. 16) under the FDI attack vector constraints as given in (Eqs 18, 19) and the load shedding vector constraints as given in (Eqs 21–23), the optimal solutions, namely the optimal FDI attack vector set ***ATK**** and the optimal load shedding vector set ***DEF**** can be obtained. Once the system loss $C(l)$ is determined, the *GARI* shown in (Eq. 15) can be used to assess the risks of the AC/DC hybrid transmission system under FDI cyber attacks.

3 Solution method

According to the modeling analysis of each stage in the aforementioned three-stage dynamic game framework, the framework can be converted into a bi-level mathematical programming problem for solution. In this paper, firstly, an IPSO algorithm is constructed to solve the lower-level programming problem, aiming to obtain the optimal FDI attack and the optimal load shedding vectors. Secondly, the payoffs of the different attack and defense fund deployment strategies can be calculated once the system loss is determined based on the solution of the lower-level programming problem.

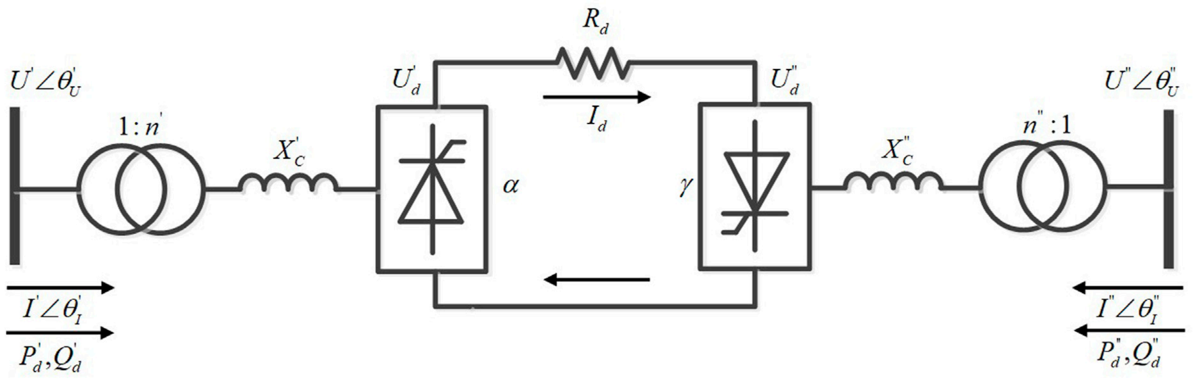


FIGURE 3
Schematic diagram of LCC-HVDC transmission model.

For the solution of the upper-level programming problem, the sub-game perfect Nash equilibrium is solved by using the BI method (Aliprantis, 1999), and it is also helpful to calculate the deployment of funds under the certain fund constraints. Finally, the risk assessment analysis is carried out in accordance with the Nash equilibrium obtained under various fund constraints.

3.1 Solution for the lower-level programming problem

It should be noted that the FDI attack against the AC state estimation system proposed in this paper is essentially a reconstruction form of partial power flow. According to the rules of generating FDI attack vectors described in Section 2.3, the tampered data and other data in the attack area still meet the power flow constraints, and only some inequality constraints such as voltage magnitude and line capacity are violated in the attack area. From the perspective of power grid dispatcher (the defender), it can be considered that the load changes cause some grid measurement data to exceed the limits. Therefore, the tampered data can bypass the bad data detector and affect the system state estimation.

As the tampered power grid data still meets the power flow constraints, the potential attack selections can be searched through the numerical relationship between power system unknowns and equations. If the number of unknowns in the set of all attacked target substations exceeds the number of equations, the set is considered to be suitable for FDI attacks, that is, a potential attack selection. On the one hand, since the active power, reactive power, voltage magnitude, and phase angle of each attacked target substation node need to be calculated, the number of unknowns $\boldsymbol{N_x}$ can be expressed as

$$\boldsymbol{N_x} = 4\boldsymbol{N}(\boldsymbol{A}) \tag{24}$$

Moreover, based on the (Eq. 18) and (Eq. 19), as well as the relationship between active power and reactive power of load, the number of the equations $\boldsymbol{N_{eq}}$ can be expressed as

$$\boldsymbol{N_{eq}} = 3\boldsymbol{N}(\boldsymbol{A}) + \boldsymbol{N}(\boldsymbol{A_g}) + \boldsymbol{N}(\boldsymbol{A_0}) + \boldsymbol{N}(\boldsymbol{A_e}) \tag{25}$$

In this paper, a depth-first search strategy (DFS) is leveraged to search for the potential attack selections, and if the number of all attacked target substation sets meets $\boldsymbol{N_x} > \boldsymbol{N_{eq}}$, it should be added to the potential attack selection set $\boldsymbol{AP} = \{\boldsymbol{A_1}, ..., \boldsymbol{A_i}, ..., \boldsymbol{A_o}\}$.

The FDI attack vectors can be constructed based on a given potential attack selection. According to (Eq. 19) and the relationship between active power and reactive power of load, it can be seen that once the active power of each attacked target substation is determined, the other three unknowns can be calculated based on the active power data, and the attack vectors can be represented by the following active power injection vectors:

$$\Delta\boldsymbol{P_{dA}} \sim \boldsymbol{ATK} \tag{26}$$

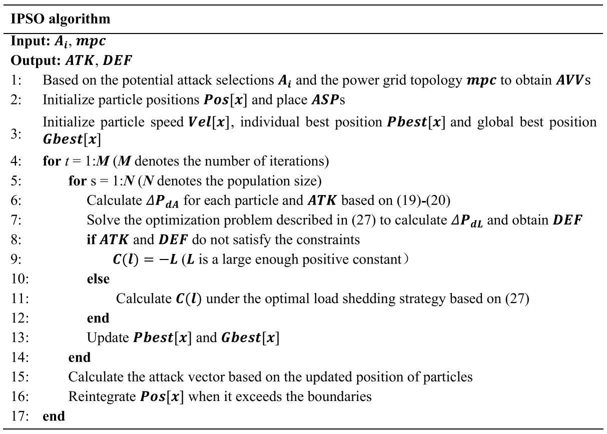
For a determined $\boldsymbol{ATK^*}$, the max-min optimization problem described in (Eq. 16) can be converted into the following single-level non-linear optimization problem.

$$\boldsymbol{C}(\boldsymbol{l}) = \min_{\boldsymbol{DEF}} \sum_{\Delta\boldsymbol{P_{dL}}\in\boldsymbol{DEF},\Delta\boldsymbol{P^*_{dA}}\in\boldsymbol{ATK^*}} \Delta\boldsymbol{P_{dL}}\left(\Delta\boldsymbol{P^*_{dA}}\right) \tag{27}$$

Subject to Eqs 21–23.

In order to solve the aforementioned problem effectively, an open-source non-linear optimization solver IPOPT (Wächter and Biegler, 2006) is employed to obtain the optimal load shedding strategy of the AC/DC hybrid transmission system. The corresponding solution $\boldsymbol{DEF}$ represents the optimal load shedding vector set corresponding to $\boldsymbol{ATK^*}$.

TABLE 2 Procedure of the proposed IPSO algorithm.



```
IPSO algorithm
Input: $A_i$, $mpc$
Output: $ATK$, $DEF$
Based on the potential attack selections $A_i$ and the power grid topology $mpc$ to obtain $AVV$s
Initialize particle positions $Pos[x]$ and place $ASP$s
Initialize particle speed $Vel[x]$, individual best position $Pbest[x]$ and global best position $Gbest[x]$
for $t = 1{:}M$ ($M$ denotes the number of iterations)
    for s = 1:$N$ ($N$ denotes the population size)
        Calculate $\Delta P_{dA}$ for each particle and $ATK$ based on (19)-(20)
        Solve the optimization problem described in (27) to calculate $\Delta P_{dL}$ and obtain $DEF$
        if $ATK$ and $DEF$ do not satisfy the constraints
            $C(l) = -L$ ($L$ is a large enough positive constant）
        else
            Calculate $C(l)$ under the optimal load shedding strategy based on (27)
        end
        Update $Pbest[x]$ and $Gbest[x]$
    end
    Calculate the attack vector based on the updated position of particles
    Reintegrate $Pos[x]$ when it exceeds the boundaries
end
```

Regarding the solution of the optimal attack vector, an IPSO is applied owing to the non-convex nonlinear characteristics of the optimization problem. It is known that the basic PSO algorithm is quite suitable for dealing with non-convex nonlinear optimization problems because of its simple implementation process and no need for gradient information (Nickabadi et al., 2011). In the PSO algorithm applied in this paper, the particles are designed as the part of the active power injection vectors ΔP_{dA}. It should be noted that the number of independent variables in this vector is $N_x - N_{eq}$, which corresponds to ΔP_{dA} one by one, so the positions of particles can be constructed as

$$X_i = (\Delta P_{dA,1}, \Delta P_{dA,2}, \cdots, \Delta P_{dA,m}), m = N_x - N_{eq} \tag{28}$$

As mentioned above, the load shedding amount of each substation mainly depends on the attack vector, line capacity, node voltage, and generator output under a malicious FDI attack scenario. By analyzing the FDI attack vector, the following characteristics can be found, that is, the node with the highest amount of load shedding generally has the largest or the second largest value of the active power attack vector, which can be used to generate some specific attack vectors as initial particles to assist the PSO algorithm to find the optimal solution and accelerate the convergence speed. Considering these characteristics of the FDI vectors, an IPSO algorithm with an initial particle generation technology proposed in this paper is applied to accelerate the convergence speed of the basic PSO algorithm. Moreover, these specific attack vectors can be called auxiliary attack vectors (AVVs). For attack selection A_i, the set of AVVs can be calculated as

$$S(AVV) = \arg\left\{\max\left(C\Delta P_{dA,k} + \left(\sum_{i\neq k} \Delta P_{dA,i}^2\right)^{\frac{1}{2}}\right), k \in A_j\right\}, C = \text{const} \gg 0 \tag{29}$$

Subject to (Eq. 18) and the relationship between active power and reactive power of load.

Here, the AVV can be transformed into the positions of particles, and the initial particle placed in these positions are called auxiliary search particle (ASP). With the help of ASP, the pseudocode of the IPSO algorithm for solving ATK and DEF is described in Table 2.

3.2 Solution for the upper-level programming problem

According to the load shedding results obtained by solving the lower-level programming problem mentioned above, the corresponding consequences caused by the coordinated physical-cyber attacks can be determined. Since the number of the attack and defense strategies under certain fund constraints is limited, it is easy to calculate all the payoffs between the attacker and the defender according to (Eq. 2), (Eqs 9–14). In this paper, once the payoffs are determined, the solution of the upper-level programming problem, namely the subgame perfect Nash equilibrium, can be obtained by using the BI method.

Considering that the proposed three-stage dynamic game framework is a zero-sum game problem, the payoff of the attacker can be expressed as

$$\begin{gathered} u_a(d_i, a_{ij}) = GARI(d_i, a_{ij}, l) = PAYOFF_{ij} \geq 0, \\ d_i \in SD, a_{ij} \in SA(d_i), 1 \leq i \leq h, 1 \leq j \leq q \end{gathered} \tag{30}$$

The payoff function of the defender can be expressed as

$$u_d(d_i, a_{ij}) = -u_a(d_i, a_{ij}) = -PAYOFF_{ij} \tag{31}$$

Then the subgame perfect Nash equilibrium can be written as

$$u_d(d^*, a^*) \geq u_d(d_i, a_{ij}), \forall (d_i, a_{ij}) \in \Omega \tag{32}$$

where

$$\Omega = \left\{(d_i, a_{ij}) \,|\, a_{ij} \in a^*(d_i)\right\}, a^*(d_i) = \arg\left\{\max_{a_{ij}\in SA(d_i)} u_a(d_i, a_{ij})\right\} \tag{33}$$

Strategy (d^*, a^*) denotes the subgame perfect Nash equilibrium.

In order to obtain the subgame perfect Nash equilibrium, the BI method is employed in this paper, which can be divided into the following two steps. In the first step, the attacker's strategy under different defense strategy options is determined, which can be formulated as

$$a^*(d_i) = \arg\left\{\max_{a_{ij}\in SA(d_i)} u_a(d_i, a_{ij})\right\} \tag{34}$$

In the second step, the defender predicts the attack strategies, so the second step can be formulated as

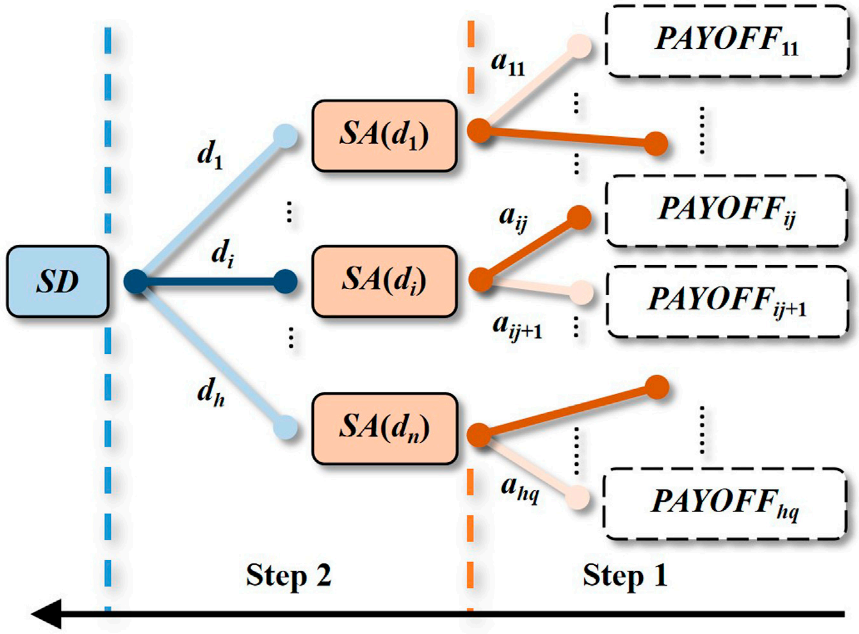


FIGURE 4
Solution process of the BI method.

$$d^{*} = \arg\left\{\max_{d_i \in SD} u_d\left(d_i, a_{ij}\right)\right\}, a_{ij} \in a^{*}\left(d_i\right) \tag{35}$$

The solution process of the BI method for the subgame perfect Nash equilibrium can be illustrated in Figure 4.

In Figure 4, the attacker first selects the corresponding optimal attack strategy (marked by the dark red branch) based on each possible defense strategy. Once the attack strategy is determined, the payoff corresponding to the defense strategy is also determined. For example, the payoff of $\boldsymbol{d_i}$ is $\boldsymbol{PAYOFF_{ij}}$ as the optimal attack strategy is $\boldsymbol{a_{ij}}$. Then, the defender selects the optimal defense strategy $\boldsymbol{d_i}$ (marked by the dark blue branch) according to the payoffs of the defense strategies. After the optimal defense and attack strategies are determined, the subgame perfect Nash equilibrium can be obtained.

Once the subgame perfect Nash equilibrium is obtained, it can be used to assess the power grid risk under the FDI attack with certain fund constraints.

3.3 Power grid risk assessment

According to the Nash equilibrium solved in the previous section, the probabilities of different strategies selected by the attacker and defender can be obtained. Therefore, the mixed attack and defense strategies can be expressed as

$$d^{*} = \left\{\left(d_i, p_d^i\right)\right\},\ a^{*} = \left\{\left(a_{ij}, p_a^j \cdot p_d^i\right)\right\}, d_i = \left(S_{Cyd}, S_{Phd}\right)^i, a_{ij} = \left(S_{Cya}, S_{Pha}\right)^{ij} \tag{36}$$

Based on the aforementioned probabilities and strategies, the expectations of fund deployment with a certain amount of fund constraints $F_m = \left(F_{Cyd}, F_{Phd}, F_{Cya}, F_{Pha}\right)$ can be calculated as

$$\begin{cases} E_{Cyd}\left(d^{*}\right) = \sum p_d^i \cdot S_{Cyd}^i \\ E_{Phd}\left(d^{*}\right) = \sum p_d^i \cdot S_{Phd}^i \\ E_{Cya}\left(a^{*}\right) = \sum p_d^i \cdot p_a^j \cdot S_{Cya}^j \\ E_{Pha}\left(a^{*}\right) = \sum p_d^i \cdot p_a^j \cdot S_{Phd}^j \end{cases} \tag{37}$$

Obviously, once the amount of funds changes, the expectation of fund deployment will also change. Therefore, the subgame perfect Nash equilibrium for various funds F_m should be solved to obtain the deployment of funds under different fund constraints. Finally, the overall expectations of fund deployment on the cyber side and the physical side, that is the power grid risk under the coordinated physical-cyber attacks, can be calculated as

$$\begin{cases} Risk_{Cy} = \dfrac{1}{N}\sum_{m=1}^{N}\left(E_{Cyd}\left(d^{*}\right) + E_{Cya}\left(a^{*}\right)\right)\Big|F_m \\ Risk_{Ph} = \dfrac{1}{N}\sum_{m=1}^{N}\left(E_{Phd}\left(d^{*}\right) + E_{Pha}\left(a^{*}\right)\right)\Big|F_m \end{cases} \tag{38}$$

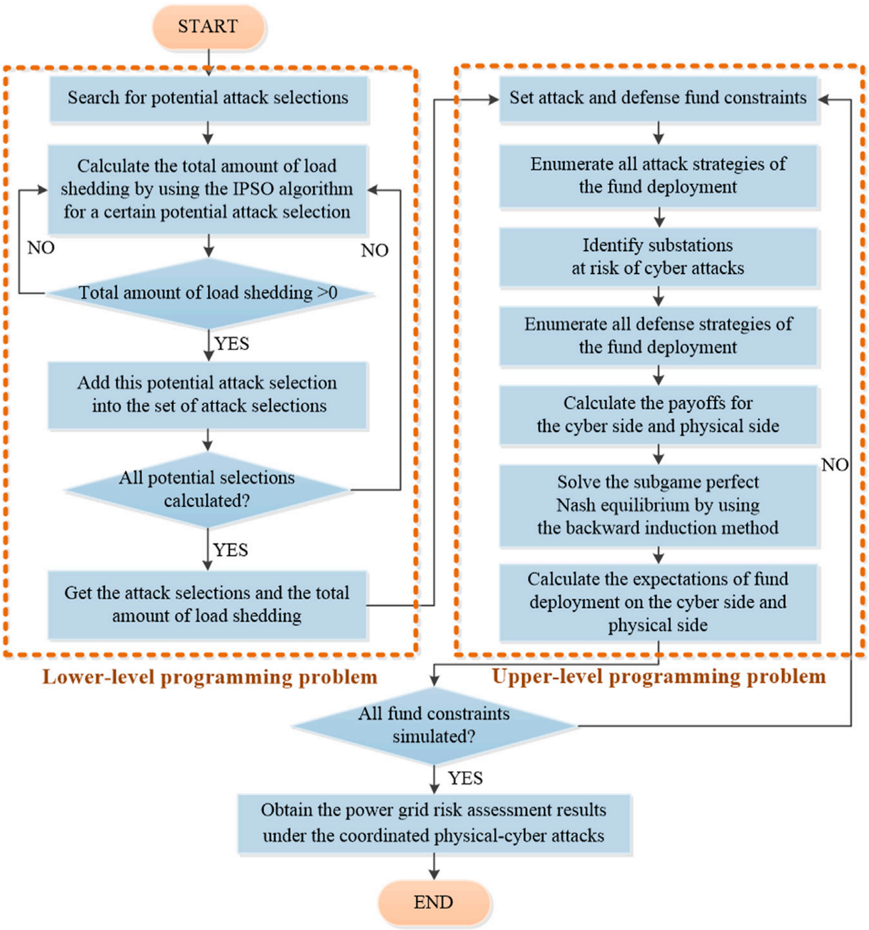

START
Search for potential attack selections
Calculate the total amount of load shedding by using the IPSO algorithm for a certain potential attack selection
NO
NO
Total amount of load shedding >0
YES
Add this potential attack selection into the set of attack selections
All potential selections calculated?
YES
Get the attack selections and the total amount of load shedding
Lower-level programming problem
Set attack and defense fund constraints
Enumerate all attack strategies of the fund deployment
Identify substations at risk of cyber attacks
Enumerate all defense strategies of the fund deployment
Calculate the payoffs for the cyber side and physical side
Solve the subgame perfect Nash equilibrium by using the backward induction method
Calculate the expectations of fund deployment on the cyber side and physical side
NO
Upper-level programming problem
All fund constraints simulated?
YES
Obtain the power grid risk assessment results under the coordinated physical-cyber attacks
END

FIGURE 5
Flow chart of the converted bi-level programing model solution.

Figure 5 illustrates the whole flow chart of the solutions for the upper-level and lower-level programming problems.

4 Case study

In this paper, the case studies are performed on a modified IEEE 14-node AC/DC hybrid transmission test system as shown in Figure 6 to verify the validity and effectiveness of the proposed model and algorithm. In the original IEEE 14-node system, the original AC transmission line between node 1 and node 5 is replaced by a ±500 kV HVDC transmission line to form an AC/DC hybrid transmission test system (Lotfjou et al., 2009). The corresponding system data including the parameters of the DC transmission line can be found in supplementary material. All simulations are performed under the Matlab™ environment, and the hardware configuration is as follows: CPU: Intel i7-10875H 8-Core, GPU: RTX 2060, RAM: 16 GB (8 GB × 2 GB) DDR4 3,200 MHz.

In this paper, the integer value of 1.25 times the rated apparent power of each line is taken as the upper bound of the capacity of the line. Meanwhile, $\boldsymbol{nATK}_{max}$ is limited to 7, and the maximum change percentage of data tampering under FDI attack is set to $\boldsymbol{\tau} = 0.5$. In the following sections, the load shedding analysis, DC line impact analysis, and system security risk analysis are elaborately conducted under the coordinated physical-cyber attacks.

4.1 Load shedding analysis under false data injection attack

According to the derivation of the potential attack selections discussed in Section 3.1, a total of 772 potential attack selections can be found under the given FDI attack constraints. However, after calculating the corresponding consequences, 770 potential attack selections will only cause the changes in power flow, and the remaining two potential

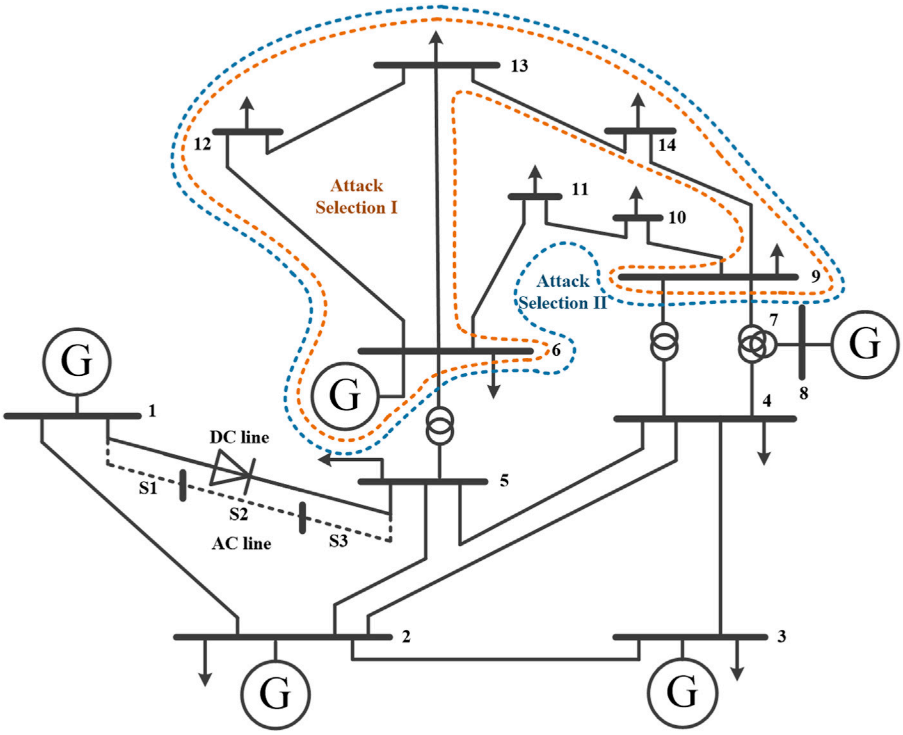


FIGURE 6
The modified IEEE14-node AC/DC hybrid transmission test system.

attack selections will lead to the load shedding. Therefore, these two attack selections are specifically utilized for load shedding analysis under FDI attack. As shown in Figure 6, there are two attack selections, namely Attack Selection I and Attack Selection II, in which the Attack Selection I contains five target substations: 6, 9, 12, 13, and 14, and the Attack Selection II contains seven target substations: 6, 9, 10, 11, 12, 13, and 14. By solving the lower programming problem described in Section 3.1, the optimal attack vector set ***ATK*** and the optimal load shedding vector set ***DEF*** corresponding to the two attack selections mentioned above are shown in Table 3 and Table 4, respectively.

From Tables 3, 4, it can be observed that under the coordinated physical-cyber attack, the total load shedding amount occurred in the Attack Selection I is 3.9511 MW, and that in the Attack Selection II is 6.8962 MW. In addition, the largest load shedding occurs at Substation 13 in the two attack selections.

In order to further validate the effectiveness of the proposed initial particle generation technology and the stability of the IPSO algorithm, the corresponding simulation analysis is carried out based on the ***ASP***. Figure 7 shows the comparison results of the total load shedding amount of the IPSO algorithm with ***ASP***, the basic PSO algorithm without ***ASP*** and the Grey Wolf Optimizer (GWO) algorithm under 50 independent trials. The population size and the number of iterations of all these algorithms are set to 30 and 20. According to the simulation results shown in Table 5, the standard deviation of the IPSO algorithm applied to the Attack Selection II is 5.8695×10^{-4}, which is much lower than that of the basic PSO algorithm and the GWO algorithm, which means that the proposed IPSO algorithm with ***ASP*** has good stability. All algorithms are accelerated by parallel computing technology with the help of the Parallel Computing Toolbox provided by MATLAB™, and the running time is shown in Table 5. Figure 8 demonstrates the corresponding convergence curves of the three algorithms mentioned above, and it can be seen that the IPSO algorithm with ***ASP*** shows a good acceleration effect.

4.2 DC transmission line impact analysis

In order to explore and exploit the impact of DC transmission line on system risk under the coordinated physical-cyber attacks, the corresponding comparative analysis is conducted between an AC transmission system and the AC/DC hybrid transmission system as shown in Figure 6 under FDI

TABLE 3 Optimal *ATK* and *DEF* corresponding to the attack selection I.

Substation	*ATK*			*DEF*	
	ΔP_{dA} (MW)	ΔQ_{dA} (Mvar)	ΔV_{mA} (p.u.)	ΔP_{dL} (MW)	ΔQ_{dL} (Mvar)
6	−1.8051	−1.2088	0	0	0
9	−0.8967	−0.5046	0	0	0
12	−3.0500	−0.8000	−0.0020	0	0
13	5.0726	2.1793	0.0036	3.9511	1.6975
14	0.6121	0.2054	0.0024	0	0

TABLE 4 Optimal *ATK* and *DEF* corresponding to the attack selection II.

Substation	*ATK*			*DEF*	
	ΔP_{dA} (MW)	ΔQ_{dA} (Mvar)	ΔV_{mA} (p.u.)	ΔP_{dL} (MW)	ΔQ_{dL} (Mvar)
6	−1.6123	−1.0797	0	0	0
9	−5.9599	−3.3537	0	0	0
10	4.5000	2.9000	0.0026	1.4371	0.9261
11	−1.7500	−0.9000	-2.37×10^{-4}	0	0
12	−3.0500	−0.8000	−0.0020	0	0
13	3.4670	1.4895	0.0035	5.4591	2.3454
14	4.2518	1.4268	0.0069	0	0

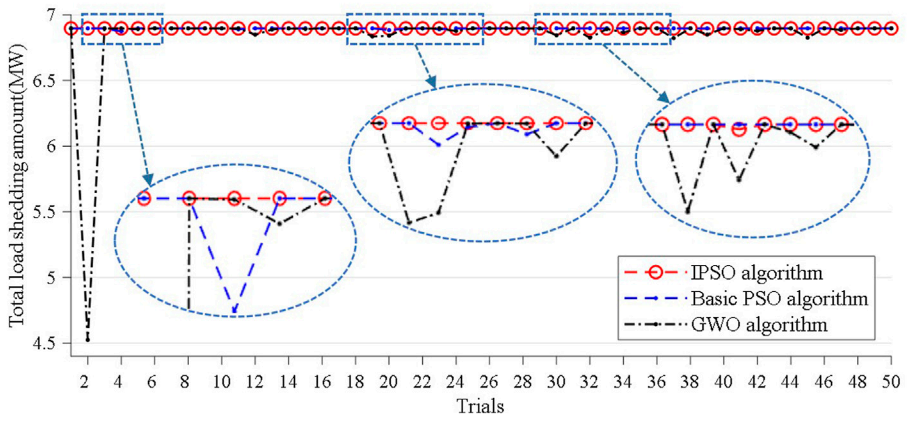


FIGURE 7
Comparison results of the total load shedding amount of three algorithms under 50 independent trials.

attacks. Regarding the AC transmission system, an AC transmission line consisting of three segments is introduced between node 1 and node 5, and the corresponding line parameters are given in Table 6. Table 7 shows the system load shedding results for the two test systems mentioned above under different attack selections. Moreover, the detailed results of the AC transmission system are provided in Supplementary Material.

It can be seen from Table 7 that when the attacker performs Attack Selection I, the total load shedding amount for the AC transmission system is 3.2388 MW, while that for the AC/DC hybrid transmission system is

TABLE 5 Simulation results of three algorithms under 50 independent trials.

Algorithm	Standard deviation (Attack Selection I)	Standard deviation (Attack Selection II)	Running time
IPSO	1.3458×10^{-15}	5.8695×10^{-4}	128–151 s
Basic PSO	1.3450×10^{-15}	3.9269×10^{-3}	136–149 s
GWO	1.3457×10^{-15}	0.33436	113–138 s

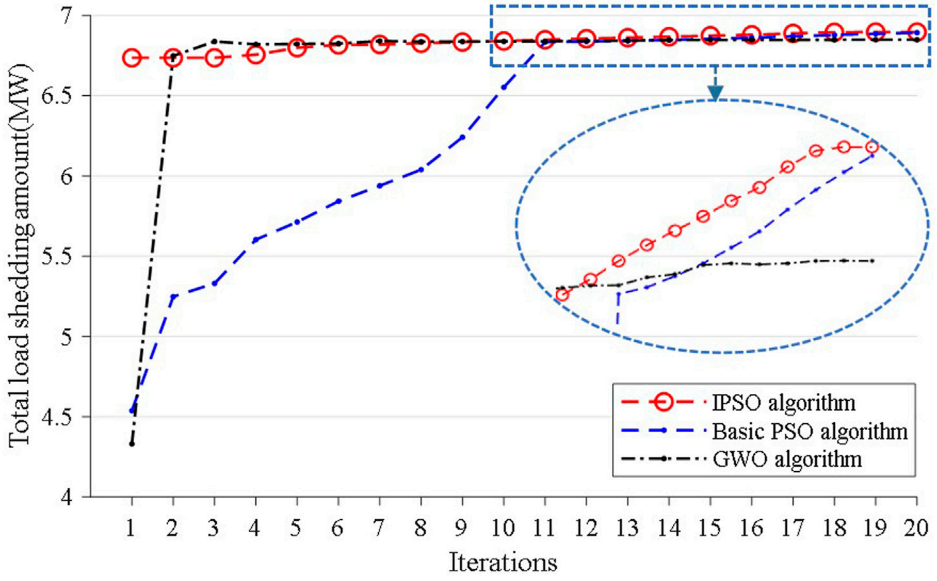


FIGURE 8
Convergence curves of three algorithms.

TABLE 6 Parameters of the AC transmission line (p.u.).

Segment	*R*	*X*	*B*	*S*
S1	0.05403	0.22304	0.0492	70MVA
S2	0.05403	0.22304	0.0492	70MVA
S3	0.05403	0.22304	0.0492	70MVA

3.9511 MW; when the attacker performs Attack Selection II, the total load shedding amount for the AC transmission system is 6.2373 MW, while that for the AC/DC hybrid transmission system is 6.8962 MW. It can also be found that when there is only a DC transmission line between node 1 and node 5, the total load shedding amount of the system caused by FDI attacks increases by 21.99% and 10.56%, respectively, compared with that when there is only an AC transmission line. Table 8 shows the operating conditions of the DC transmission line before and after the FDI attacks.

It can be found from Table 8 that only the ignition angle changes relatively after the attacker makes the Attack Selection II, and the other measurement data of the DC transmission line are basically not affected by the coordinated physical-cyber attacks. Since the data of DC transmission lines are considered to be untampered, the impact of the corresponding coordinated physical-cyber attack on the measurement data of the DC transmission lines is not significant. Thus, if the attacker could not directly tamper with the data of DC transmission lines, it is difficult to cause the DC blocking.

To sum up, it can be concluded that even if the DC transmission lines can be prevented from cyber attacks, the FDI attacks can still pose threat to the AC/DC hybrid transmission system, so it is necessary to conduct the security risk assessment.

TABLE 7 System load shedding results.

System	Attack Selection I (MW)	Attack Selection II (MW)
AC transmission system	3.2388	6.2373
AC/DC hybrid transmission system	3.9511	6.8962

TABLE 8 Operating conditions of the DC transmission line before and after FDI attacks.

Before FDI attack				
Rec	α = 21.89°	$U_d^{'}$ = 500.84kV	$P_d^{'}$ = 65.11kW	$Q_d^{'}$ = 26.16kW
Inv	γ = 18.00°	$U_d^{''}$ = 500.25kV	$P_d^{''}$ = −65.03kW	$Q_d^{''}$ = 21.13kW
After FDI attack (Attack Selection I)				
Rec	α = 20.61°	$U_d^{'}$ = 501.47kV	$P_d^{'}$ = 65.19kW	$Q_d^{'}$ = 24.52kW
Inv	γ = 18.00°	$U_d^{''}$ = 500.89kV	$P_d^{''}$ = −65.12kW	$Q_d^{''}$ = 21.16kW
After FDI attack (Attack Selection II)				
Rec	α = 18.64°	$U_d^{'}$ = 502.08kV	$P_d^{'}$ = 65.27kW	$Q_d^{'}$ = 22.02kW
Inv	γ = 18.00°	$U_d^{''}$ = 501.50kV	$P_d^{''}$ = −65.19kW	$Q_d^{''}$ = 21.18kW

4.3 System security risk analysis

Based on the risk assessment framework described in Section 2, the comprehensive system security risk is conducted in this section. In (Eq. 11), the inherent risk value $\boldsymbol{\mu}$ of substation communication network is set to \$3K, \$6K, \$4K, \$8K, \$7K, \$6K, \$5K, \$2K, \$7K, \$5K, \$5K, \$5K, \$6K, and \$5K in the order of substation numbers. Considering that the deployment strength of substation security forces is usually similar, the inherent risk value $\boldsymbol{\lambda}$ of substation security forces in (Eq. 12) is set to \$100K. For the defender, $\boldsymbol{CydL_1}$ is set to \$10K, $\boldsymbol{CydL_2}$ is set to \$20K, $\boldsymbol{PhdL_1}$ is set to \$50K, and $\boldsymbol{PhdL_2}$ is set to \$100K. For the attacker, $\boldsymbol{CyaL_1}$ is set to \$10K, $\boldsymbol{CyaL_2}$ is set to \$20K, $\boldsymbol{PhaL_1}$ is set to \$50K, and $\boldsymbol{PhaL_2}$ is set to \$100K. According to the maximum amount of funds, the range of $\boldsymbol{F_{Cyd}}$ should be from \$70K to \$100K, the range of $\boldsymbol{F_{Phd}}$ should be from \$250K to \$400K, the range of $\boldsymbol{F_{Cya}}$ should be from \$70K to \$100K, and the range of $\boldsymbol{F_{Pha}}$ should be from \$350K to \$500K.

Based on the above parameter settings, the corresponding system security risk analysis is carried out, and the following simulation cases are analyzed and discussed elaborately.

1) Case 1: The relatively low budget of defense and attack funds, that is, $\boldsymbol{F_{Cyd}}$, $\boldsymbol{F_{Phd}}$, $\boldsymbol{F_{Cya}}$, and $\boldsymbol{F_{Pha}}$ take relatively low values;
2) Case 2: The relatively high budget of defense and attack funds, that is, $\boldsymbol{F_{Cyd}}$, $\boldsymbol{F_{Phd}}$, $\boldsymbol{F_{Cya}}$, and $\boldsymbol{F_{Pha}}$ take relatively high values;
3) Case 3: The budget of defense and attack funds is within a certain range, that is, $\boldsymbol{F_{Cyd}}$, $\boldsymbol{F_{Phd}}$, $\boldsymbol{F_{Cya}}$, and $\boldsymbol{F_{Pha}}$ take the specified range.

In case 1, $\boldsymbol{F_{Cyd}}$, $\boldsymbol{F_{Phd}}$, $\boldsymbol{F_{Cya}}$, and $\boldsymbol{F_{Pha}}$ are set to \$70K, \$250K, \$70K, and \$350K, respectively. In this case, the total number of defense strategies is 104538, and the total number of attack strategies is 101. The corresponding subgame perfect Nash equilibrium pertinent to the fund allocation of the attacker and the defender is shown in Table 9.

From Table 9, it can be found that the attacker will choose the attack strategies performed at Attack Selection I. The active power loss expectation of the test system under the current funding limitations is 1.5919 × 10^{-5} MW. From the analysis of attack and defense funds on the cyber side, the total expectations of both sides of the attack and defense deployment funds for the substation 9 are tied for the highest, all of which are \$40K. Accordingly, this substation is considered to be the most risky substation on the cyber side, and more attention should be paid to its communication network vulnerabilities. Similarly, on the physical side, it is also found that the substation 9 has the highest expectation for the total amount of funds deployed by the attacker and the defender, which is \$150K. This means that the risk of this substation is also the highest, so special attention should be paid to its guard force. To sum up, under these fund constraints, the substations 9 is identified as the critical substation of the test system in this case. Moreover, it can be observed that the attacker tends to deploy more funds on the substation with stronger defense on cyber side to increase the success probability of a coordinated physical-cyber attack.

In case 2, $\boldsymbol{F_{Cyd}}$, $\boldsymbol{F_{Phd}}$, $\boldsymbol{F_{Cya}}$, and $\boldsymbol{F_{Pha}}$ are set to \$80K, \$300K, \$90K, and \$400K, respectively. In this case, the total number of defense strategies is 127,449, and the total number of attack strategies is 197. The corresponding subgame perfect Nash equilibrium pertinent to the fund allocation of the attacker and the defender is shown in Table 10.

From Table 10, it can be found that the active power loss expectation of the test system under the current funding limitations is 1.9777 × 10^{-5} MW. From the analysis of attack and defense funds on the cyber side, the total expectations of both sides of the attack and defense deployment funds for substations 9, 12, and 14 are tied for the highest, all of which are \$40K. Accordingly, these three substations are considered to be the most risky substations on the cyber side, and more attention should be paid to their communication network vulnerabilities. Similarly, on the physical side, it is also found that the three substations have the highest expectations for the total amount of funds deployed by the attacker and the defender, which is \$150K. This means that the risks of these three substations are also the highest, so special attention should be

TABLE 9 Subgame perfect Nash equilibrium under specific fund constraints.

Strategy	Substation	Fund on cyber side ($K)	Fund on physical side ($K)	Probability (%)
DEF #13842	{6,9,12,13,14}	{20,20,10,10,10}	{50,50,50,50,50}	50
--- ATK #100	{6,9,12,13,14}	{20,20,10,10,10}	{100,100,50,50,50}	100
DEF #36718	{6,9,12,13,14}	{10,20,10,20,10}	{50,50,50,50,50}	50
--- ATK #45	{6,9,12,13,14}	{10,20,10,20,10}	{50,100,50,100,50}	100

TABLE 10 Subgame perfect Nash equilibrium under specific fund constraints.

Strategy	Substation	Fund on cyber side ($K)	Fund on physical side ($K)	Probability (%)
DEF #90037	{6,9,12,13,14}	{10,20,20,10,20}	{50,50,100,50,50}	50
--- ATK #8	{6,9,12,13,14}	{10,20,20,20,20}	{100,100,50,50,100}	50
--- ATK #32	{6,9,12,13,14}	{20,20,20,10,20}	{50,100,50,100,100}	50
DEF #90067	{6,9,12,13,14}	{10,20,20,10,20}	{50,50,50,50,100}	50
--- ATK #10	{6,9,12,13,14}	{10,20,20,20,20}	{100,100,100,50,50}	50
--- ATK #34	{6,9,12,13,14}	{20,20,20,10,20}	{50,100,100,100,50}	50

TABLE 11 Overall expectations of the fund deployment of attacker and defender.

Substation	BUS 6	BUS 9	BUS 12	BUS 13	BUS 14	Others
Funds on cyber side	$33691.4	$31250.0	$35452.5	$34433.6	$35172.5	0
Funds on physical side	$ 150048.8	$144335.9	$152311.2	$151123.0	$152181.0	0

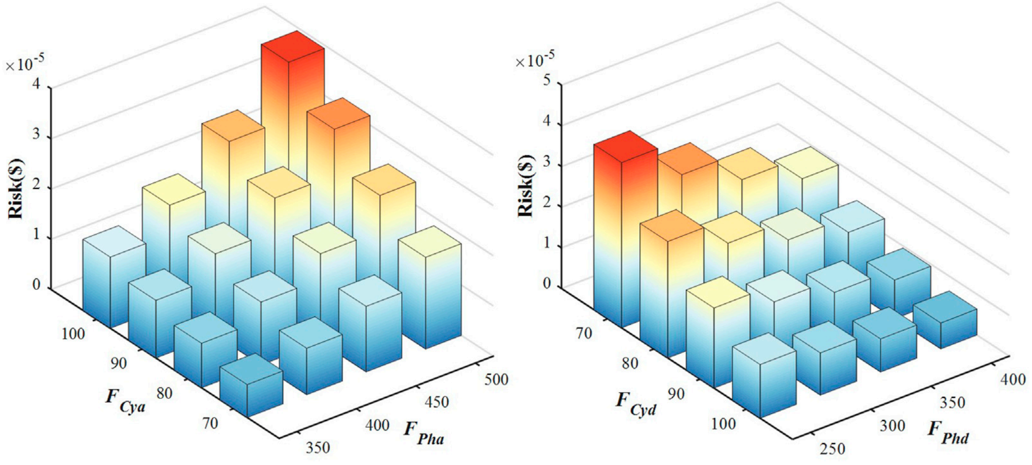


FIGURE 9
The impact of changes in attack and defense funds on the risk expectations of the test system.

paid to their guard forces. To sum up, under these fund constraints, substations 9, 12, and 14 are identified as the critical substations of the test system in this case. Moreover, it can be observed that the attacker tends to deploy more funds on the substation with weaker defense on physical side to increase the probability of a successful coordinated physical-cyber attack.

In case 3, F_{Cyd}, F_{Phd}, F_{Cya}, and F_{Pha} take the specified range as mentioned above. After obtaining all the subgame perfect Nash equilibriums of the defense and attack budget within a certain range, and according to (Eq. 38), the overall expectations of the fund deployment of the attacker and the defender can be calculated as shown in Table 11.

From Table 11, it can be seen that the overall expectation of the fund deployment on the cyber side pertinent to the substation 12 is the highest, which means that the cyber side of the substation 12 is the most critical, and it is necessary to strictly investigate the vulnerabilities in the communication network. Meanwhile, the overall expectation of the fund deployment on the physical side pertinent to the substation 12 is the highest, which means that the physical side of the substation 12 is also the most critical, and it is necessary to strictly control the personnel entering and leaving the station, as well as to check the illegal monitoring equipment regularly. To sum up, the substation 12 is identified as the critical substation in the test system.

Figure 9 illustrates the impact of changes in attack and defense funds on the risk expectations of the test system. It can be found that from the attacker's perspective, the more funds invested in the attack, the higher the risk of the test system caused by the attack. In particular, the more funds invested on the cyber side, the more effective the attack. Similarly, from the defender's perspective, the more funds invested in the defense, the lower the risk of the test system, and the more funds invested on the cyber side, the better the defense effect, which provides a significant reference for power grid dispatcher to deploy the optimal defense funds.

5 Conclusion

This paper investigates the inherent vulnerability of AC/DC hybrid transmission system under the physical-cyber coordinated attacks, and a three-stage physical-cyber attack and defense risk assessment framework based on dynamic game theory is proposed. In the proposed framework, the corresponding deployment of defense funds in stage 1, the deployment of attack funds in stage 2 including how to quantify the success probability of the FDI attack on the substation, and the action of the defender including how to model the FDI attack strategy based on AC state estimation, are analyzed elaborately and carefully. Finally, the dynamic game risk assessment framework is converted into a bi-level programming problem, and the classic BI associated with an IPSO algorithm is applied for the solution of the problem. The simulation results performed on a modified IEEE 14-node AC/DC hybrid transmission test system demonstrate that under the coordinated physical-cyber attacks, the optimal $\boldsymbol{ATK}$ and $\boldsymbol{DEF}$ can be obtained, leading to different load shedding amount in different attack selections. In addition, the FDI attacks pose a greater threat to the AC/DC hybrid transmission system compared with the AC transmission system, and the inherent weakness of the AC/DC hybrid transmission system can be effectively identified through conducting the risk assessment with different budgets of defense and attack funds.

In the near future, the impact of high proportion of grid-connected clean energy on the system risk will be further investigated under the coordinated physical-cyber attacks.

Data availability statement

The datasets presented in this study can be found in online repositories. The names of the repository/repositories and accession number(s) can be found in the article/Supplementary Material.

Author contributions

XL performed the model analysis and algorithm experiment, as well as wrote the manuscript. LS contributed to the model framework and revised the manuscript.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Supplementary material

The Supplementary Material for this article can be found online at: https://www.frontiersin.org/articles/10.3389/fenrg.2022.1082442/full#supplementary-material

References

Aliprantis, C. D. (1999). On the backward induction method. *Econ. Lett.* 64 (2), 125–131. doi:10.1016/S0165-1765(99)00068-3

Amir, G., Mohammad, M., Anurag, K. S., and Ali, M. S. (2019). "Cyber-physical vulnerability and security analysis of power grid with HVDC line (S. 1-6)," in 2019 North American Power Symposium (NAPS). doi:10.1109/NAPS46351.2019.9000209

Che, L., Liu, X., and Li, Z. (2018). Mitigating false data attacks induced overloads using a corrective dispatch scheme. *IEEE Trans. Smart Grid* 10 (3), 3081–3091. doi:10.1109/TSG.2018.2817515

Chung, H. M., Li, W. T., Yuen, C., Chung, W. H., Zhang, Y., and Wen, C. K. (2018). Local cyber-physical attack for masking line outage and topology attack in smart grid. *IEEE Trans. Smart Grid* 10 (4), 4577–4588. doi:10.1109/TSG.2018.2865316

Dai, Q., and Shi, L. (2020). "A game-theoretic analysis of cyber attack-mitigation in centralized feeder automation system," in 2020 IEEE Power Energy Society General Meeting (PESGM). doi:10.1109/PESGM41954.2020.9281583

Gao, B., and Shi, L. (2020). Modeling an attack-mitigation dynamic game-theoretic scheme for security vulnerability analysis in a cyber-physical power system. *IEEE Access* 8, 30322–30331. doi:10.1109/ACCESS.2020.2973030

Gao, B., Shi, L., and Ni, Y. (2019). "A dynamic defense-attack game scheme with incomplete information for vulnerability analysis in a cyber-physical power infrastructure," in 8th Renewable Power Generation Conference. doi:10.1049/cp.2019.0285

Hasan, S., Dubey, A., Karsai, G., and Koutsoukos, X. (2020). A game-theoretic approach for power systems defense against dynamic cyber-attacks. *Int. J. Electr. Power & Energy Syst.* 115, 105432. doi:10.1016/j.ijepes.2019.105432

Khanna, K., Panigrahi, B. K., and Joshi, A. (2017). Bi-level modelling of false data injection attacks on security constrained optimal power flow. *IET Generation, Transm. Distribution* 11 (14), 3586–3593. doi:10.1049/iet-gtd.2017.0226

Kundur, P. S., and Malik, O. P. (2022). *Power system stability and control.* McGraw-Hill Education. https://www.accessengineeringlibrary.com/content/book/9781260473544.

Lakshminarayana, S., Belmega, E. V., and Poor, H. V. (2021). Moving-target defense against cyber-physical attacks in power grids via game theory. *IEEE Trans. Smart Grid* 12 (6), 5244–5257. doi:10.1109/TSG.2021.3095083

Liang, G., Weller, S. R., Zhao, J., Luo, F., and Dong, Z. Y. (2016). The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE Trans. Power Syst.* 32 (4), 3317–3318. doi:10.1109/TPWRS.2016.2631891

Liu, X., and Li, Z. (2016). False data attacks against AC state estimation with incomplete network information. *IEEE Trans. Smart Grid* 8 (5), 2239–2248. doi:10.1109/TSG.2016.2521178

Liu, Z., and Wang, L. (2021). FlipIt game model-based defense strategy against cyberattacks on SCADA systems considering insider assistance. *IEEE Trans. Inf. Forensics Secur.* 16, 14. doi:10.1109/TIFS.2021.3065504

Lotfjou, A., Shahidehpour, M., Fu, Y., and Li, Z. (2009). Security-constrained unit commitment with AC/DC transmission systems. *IEEE Trans. Power Syst.* 25 (1), 531–542. doi:10.1109/TPWRS.2009.2036486

National institute of standards and technology (2022). Nvd - vulnerabilities. https://nvd.nist.gov/vuln (Accessed October 1, 2022).

Nickabadi, A., Ebadzadeh, M. M., and Safabakhsh, R. (2011). A novel particle swarm optimization algorithm with adaptive inertia weight. *Appl. Soft Comput.* 11 (4), 3658–3670. doi:10.1016/j.asoc.2011.01.037

Qiu, W., Sun, K., Yao, W., Wang, W., Tang, Q., and Liu, Y. (2021). Hybrid data-driven based HVdc ancillary control for multiple frequency data attacks. *IEEE Trans. Industrial Inf.* 17 (12), 8035–8045. doi:10.1109/TII.2021.3063270

Rahman, M. A., and Mohsenian-Rad, H. (2013). "False data injection attacks against nonlinear state estimation in smart power grids," in 2013 IEEE Power & Energy Society General Meeting. doi:10.1109/PESMG.2013.6672638

Ranjbar, M. H., Kheradmandi, M., and Pirayesh, A. (2019). Assigning operating reserves in power systems under imminent intelligent attack threat. *IEEE Trans. Power Syst.* 34 (4), 2768–2777. doi:10.1109/TPWRS.2019.2897595

Sanjab, A., and Saad, W. (2016). Data injection attacks on smart grids with multiple adversaries: A game-theoretic perspective. *IEEE Trans. Smart Grid* 7 (4), 2038–2049. doi:10.1109/TSG.2016.2550218

Shan, X. G., and Zhuang, J. (2020). A game-theoretic approach to modeling attacks and defenses of smart grids at three levels. *Reliab. Eng. Syst. Saf.* 195, 106683. doi:10.1016/j.ress.2019.106683

Shao, C. W., and Li, Y. F. (2021). Optimal defense resources allocation for power system based on bounded rationality game theory analysis. *IEEE Trans. Power Syst.* 36 (5), 4223–4234. doi:10.1109/TPWRS.2021.3060009

Tian, M., Dong, Z., and Wang, X. (2021). Analysis of false data injection attacks in power systems: A dynamic bayesian game-theoretic approach. *ISA Trans.* 115, 108–123. doi:10.1016/j.isatra.2021.01.011

Wächter, A., and Biegler, L. T. (2006). On the implementation of an interior-point filter line-search algorithm for large-scale nonlinear programming. *Math. Program.* 106 (1), 25–57. doi:10.1007/s10107-004-0559-y

Wang, K., Du, M., Maharjan, S., and Sun, Y. (2017). Strategic honeypot game model for distributed denial of service attacks in the smart grid. *IEEE Trans. Smart Grid* 8 (5), 2474–2482. doi:10.1109/TSG.2017.2670144

Wang, Q., Tai, W., Tang, Y., Ni, M., and You, S. (2019). A two-layer game theoretical attack-defense model for a false data injection attack against power systems. *Int. J. Electr. Power & Energy Syst.* 104, 169–177. doi:10.1016/j.ijepes.2018.07.007

Wei, L., Sarwat, A. I., and Saad, W. (2016). Stochastic games for power grid protection against coordinated cyber-physical attacks. *IEEE Trans. Smart Grid* 9 (2), 684–694. doi:10.1109/TSG.2016.2561266

Xiang, Y., Wang, L., and Zhang, Y. (2018). Adequacy evaluation of electric power grids considering substation cyber vulnerabilities. *Int. J. Electr. Power & Energy Syst.* 96, 368–379. doi:10.1016/j.ijepes.2017.10.004

Xu, L., Guo, Q., Sheng, Y., Muyeen, S. M., and Sun, H. (2021). On the resilience of modern power systems: A comprehensive review from the cyber-physical perspective. *Renew. Sustain. Energy Rev.* 152, 111642. doi:10.1016/j.rser.2021.111642

Yuan, Y., Li, Z., and Ren, K. (2011). Modeling load redistribution attacks in power systems. *IEEE Trans. Smart Grid* 2 (2), 382–390. doi:10.1109/TSG.2011.2123925

Zhang, Z., Huang, S., Chen, Y., Li, B., and Mei, S. (2021). Cyber-physical coordinated risk mitigation in smart grids based on attack-defense game. *IEEE Trans. Power Syst.* 37 (1), 530–542. doi:10.1109/TPWRS.2021.3091616

Nomenclature

$\boldsymbol{d}, \boldsymbol{a}, \boldsymbol{l}$ Defense strategy, attack strategy, and system dispatching strategy

$\boldsymbol{SD}$ Set of defense strategies in Stage 1

$\boldsymbol{SA}(\boldsymbol{d})$ Set of attack strategies in Stage 2, which is impacted by defense strategy $\boldsymbol{d}$

$\boldsymbol{SL}(\boldsymbol{d}, \boldsymbol{a})$ Set of defender's actions in Stage 3, which is dependent on the strategy of both defender and attacker

$\boldsymbol{V}(\boldsymbol{d}, \boldsymbol{a})$ Vulnerability of the substation under coordinated physical-cyber attacks

$\boldsymbol{C}(\boldsymbol{l})$ Consequences caused by coordinated physical-cyber attacks

$\boldsymbol{S_{Cyd}}$ Allocation of funds for cyber defense security

$\boldsymbol{Cyd_i}$ Cyber security funds requested by the i^{th} substation

$\boldsymbol{B}$ Set of all substations

$\boldsymbol{F_{Cyd}}$ Upper limit of defense funds deployed on the cyber side

$\boldsymbol{CydL_1}$ Maintenance fund for communication network

$\boldsymbol{CydL_2}$ Funds to upgrade the cyber equipment

$\boldsymbol{S_{Phd}}$ Allocation of funds for physical security

$\boldsymbol{Phd_i}$ Physical security funds requested by the i^{th} substation

$\boldsymbol{F_{Phd}}$ Upper limit of defense funds deployed on the physical side

$\boldsymbol{PhdL_1}$ Funds to hire security guards

$\boldsymbol{PhdL_2}$ Funds to hire a professional security team for the physical security of the i^{th} substation

$\boldsymbol{S_{Cya}}$ Allocation of funds for cyber attacks

$\boldsymbol{Cya_i}$ Funds required to hire hackers for attacking the i^{th} target substation

$\boldsymbol{A}$ Set of all target substations

$\boldsymbol{F_{Cya}}$ Maximum amount of funds spent by the attack team to hire hackers

$\boldsymbol{CyaL_1}$ Hacking service fees for hiring hackers with general skill level

$\boldsymbol{CyaL_2}$ Hacking service fees for hiring hackers with high skill level

$\boldsymbol{S_{Pha}}$ Allocation of funds for physical monitoring

$\boldsymbol{Pha_i}$ Funds required to monitor the i^{th} target substation

$\boldsymbol{F_{Pha}}$ Maximum amount of funds spent by the attack team for bribery and monitoring

$\boldsymbol{PhaL_1}$ Funds spent on general monitoring

$\boldsymbol{PhaL_2}$ Funds spent on high intensity monitoring

$\boldsymbol{p_{Cy,i}}$ Probability of an attacker successfully attacking the i^{th} substation

$\boldsymbol{p_{BAG,i}}$ Probability that the attacker uses the intelligent device to tamper with data in the i^{th} substation

$\boldsymbol{p_{con,i}}$ Connectivity probability for the attacker to achieve an attack when the defender deploys cyber defense funds

$\boldsymbol{p_{Ph,i}}$ Probability of obtaining SSH port and password by non-network intrusion

$\boldsymbol{p}(\mathbf{SSH})$ Probability of an attacker getting the right SSH port number

$\boldsymbol{p}(\mathbf{Log})$ Success probability of an attacker cracking the password

$\boldsymbol{p}(\mathbf{DB})$ Probability of an attacker obtaining the right to falsify the data

$\boldsymbol{\mu}$ Inherent risk of substation communication network

$\boldsymbol{\lambda}$ Inherent risk of substation security forces

$\boldsymbol{d'}$ Determined defense strategies in the Stage 1

$\boldsymbol{a'}$ Determined attack strategies in the Stage 2

$\boldsymbol{ATK}$ Set of attack vectors

$\boldsymbol{DEF}$ Set of load shedding vectors

$\Delta\boldsymbol{P_{dL}}$ Amount of load shedding

$\Delta\boldsymbol{P_{dA}}$ Active power attack vector

$\Delta\boldsymbol{Q_{dA}}$ Reactive power attack vector

$\Delta\boldsymbol{V_{mA}}$ Voltage magnitude attack vector

$\Delta\boldsymbol{\theta_A}$ Voltage phase angle attack vector

$\boldsymbol{nATK_{max}}$ Maximum number of attacked substations

$\boldsymbol{\tau}$ Maximum percentage of data tampering changes

$\boldsymbol{P_{d,i}}$ Active load of the i^{th} substation before the coordinated physical-cyber attack

$\boldsymbol{Q_{d,i}}$ Reactive load of the i^{th} substation before the coordinated physical-cyber attack

$\boldsymbol{V_{m,i}}$ Voltage magnitude of the i^{th} substation before the coordinated physical-cyber attack

$\boldsymbol{\theta_i}$ Voltage phase angle of the i^{th} substation before the coordinated physical-cyber attack

$\boldsymbol{A}$ Set of target substations (nodes) attacked

$\boldsymbol{A_g}$ Set of generator nodes attacked

$\boldsymbol{A_0}$ Set of zero-load nodes attacked

$\boldsymbol{A_e}$ Set of edge nodes attacked

$\boldsymbol{P_{gA}}$ Active powers of the generators connecting to target substations attacked

$\boldsymbol{Q_{gA}}$ Reactive powers of the generators connecting to target substations attacked

$\boldsymbol{PartLF}$ Power flow constraints of the attacked part of the power grid

$\boldsymbol{nA}$ Number of the attacked nodes

$\boldsymbol{P_i}$ Active powers injected at the i^{th} node

$\boldsymbol{Q_i}$ Reactive powers injected at the i^{th} node

$\boldsymbol{g_{ij}}$ Conductance between the i^{th} node and the j^{th} node

$\boldsymbol{b_{ij}}$ Susceptance between the i^{th} node and the j^{th} node

$\boldsymbol{P_{g,i}}$ Total active power output of the generators connecting to the i^{th} substation

$\boldsymbol{Q_{g,i}}$ Total reactive power output of the generators connecting to the i^{th} substation

$\boldsymbol{P_{leq}}$, $\boldsymbol{Q_{leq}}$ Two equivalent injected power vectors, namely the power flow on the line connected to the attacked node and the non-attacked node

$\boldsymbol{V_{m\min,i}}$ Lower bound of the voltage magnitude of the i^{th} substation

$\boldsymbol{V_{m\max,i}}$ Upper bound of the voltage magnitude of the i^{th} substation

$\boldsymbol{\theta_{\min,i}}$ Lower bound of the voltage phase angle of the i^{th} substation

$\boldsymbol{\theta_{\max,i}}$ Upper bound of the voltage phase angle of the i^{th} substation

$\boldsymbol{S_{l,ij}}$ Apparent power of the line connecting to the i^{th} substation and the j^{th} substation

$\boldsymbol{S_{l\max,ij}}$ Upper bound of the apparent power of the line connecting to the i^{th} substation and the j^{th} substation

$\boldsymbol{P_{g\,min,i}}$ Lower bound of the total active power output of the generators connecting to the i^{th} substation

$\boldsymbol{P_{g\,max,i}}$ Upper bound of the total active power output of the generators connecting to the i^{th} substation

$\boldsymbol{Q_{g\,min,i}}$ Lower bound of the total reactive power output of the generators connecting to the i^{th} substation

$\boldsymbol{Q_{g\,max,i}}$ Upper bound of the total reactive power output of the generators connecting to the i^{th} substation

$\boldsymbol{LF}$ AC/DC power flow constraints

$\boldsymbol{nB}$ Number of the substations in the AC/DC hybrid transmission power system

$\boldsymbol{U_d^{'}}$ DC voltages of the rectifier

$\boldsymbol{U_d^{''}}$ DC voltages of the inverter

$\boldsymbol{n'}, \boldsymbol{n^{''}}$ Equivalent tap ratios

$\boldsymbol{X_C^{'}}, \boldsymbol{X_C^{''}}$ Equivalent reactance

$\boldsymbol{\alpha}$ Ignition angle

$\boldsymbol{\gamma}$ Extinction angle

$\boldsymbol{R_d}$ Equivalent resistance of the DC line

$\boldsymbol{I_d}$ Current on the DC line

$\boldsymbol{P_d^{'}}$ Active power from the rectifier to the inverter

$\boldsymbol{P_d^{''}}$ Active power from the power grid to the inverter

$\boldsymbol{Q_d^{'}}$ Reactive power consumed by the rectifier

$\boldsymbol{Q_d^{''}}$ Reactive power consumed by the inverter

$\boldsymbol{U'\angle\theta_U^{'}}$ AC phase-to-phase voltage of the rectifier

$\boldsymbol{U^{''}\angle\theta_U^{'}}$ AC phase-to-phase voltage of the inverter

$\boldsymbol{I'\angle\theta_I^{'}}$ AC current of the rectifier

$\boldsymbol{I^{''}\angle\theta_I^{''}}$ AC current of the inverter

$\boldsymbol{N_x}$ Number of unknowns

$\boldsymbol{N_{eq}}$ Number of equations

$\boldsymbol{N(\bullet)}$ Number of elements in the set $\bullet$

$\boldsymbol{o}$ Number of the potential attack selections

$\boldsymbol{AP}$ Potential attack selection set

$\boldsymbol{m}$ Value of $\boldsymbol{N_x - N_{eq}}$

$\boldsymbol{X_i}$ Position of the i^{th} particle

$\boldsymbol{AVV}$ Auxiliary attack vector

$\boldsymbol{ASP}$ Auxiliary search particle

$\boldsymbol{M}$ Number of iterations

$\boldsymbol{N}$ Population size

$\boldsymbol{d_i}$ The i^{th} defense strategy based on (5)

$\boldsymbol{a_{ij}}$ The j^{th} attack strategy based on (8) which is impacted by $\boldsymbol{d_i}$ in Stage 1

$\boldsymbol{PAYOFF_{ij}}$ Value of the payoff when the defender selects the i^{th} defense strategy in Stage 1 and the attacker selects the j^{th} attack strategy in Stage 2

$\boldsymbol{SA(d_i)}$ Set of attack fund deployment strategies affected by the defense fund deployment strategy $\boldsymbol{d_i}$

$\boldsymbol{h}$ Number of defense strategies

$\boldsymbol{q}$ Number of attack strategies

$\boldsymbol{a^*(d_i)}$ Optimal attack strategies based on the defense strategies decided in Stage 1

$\boldsymbol{(d^*, a^*)}$ Subgame perfect Nash equilibrium

$\boldsymbol{p_d^i}$ Probability of using defense strategy $\boldsymbol{d_i}$

$\boldsymbol{p_a^j}$ Probability of using attack strategy $\boldsymbol{a_{ij}}$ when the defender decides to use the defense strategy $\boldsymbol{d_i}$ in the Stage 1

$\boldsymbol{F_m}$ Fund constraints

$\boldsymbol{E_{Cyd}(d^*)}$ Expectation of the defense funds on the cyber side

$\boldsymbol{E_{Phd}(d^*)}$ Expectation of the defense funds on the physical side

$\boldsymbol{E_{Cya}(a^*)}$ Expectation of the attack funds on the cyber side

$\boldsymbol{E_{Pha}(a^*)}$ Expectation of the attack funds on the physical side

$\boldsymbol{Risk_{Cy}}$ Expectation of funds invested by the attacker and defender on the cyber side

$\boldsymbol{Risk_{Ph}}$ Expectation of funds invested by the attacker and defender on the physical side